

EXHIBIT A

20 MAG 19 03

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States of America for a Search Warrant for A Silver Samsung Phone with Silver Case (Including Any SIM Cards or Other Memory Cards Contained Therein), and a Silver Samsung Phone with Serial Number R28J425GCTV, (Including Any SIM Cards or Other Memory Cards Contained Therein), Inventoried by the FBI in connection with the Arrest of MUSTAPHA RAJI, on or about December 20, 2019; USAO 2018R01109

TO BE FILED UNDER SEAL

**Agent Affidavit in Support of
Application for Search and Seizure
Warrant**

SOUTHERN DISTRICT OF NEW YORK) ss.:

MICHAEL MULLOY, Detective with the Suffolk County Police Department and Task Force Officer with the Federal Bureau of Investigation, being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I have been a Task Force Officer with the Federal Bureau of Investigation, ("FBI") for approximately 3 years. I am currently assigned to a cyber intrusion squad at FBI's New York Field Office. I have participated in investigations into criminal offenses involving computer and wire fraud, and am familiar with the means and methods used to commit such offenses. In that capacity, I have received training in the review of electronic evidence and have participated in the execution of search warrants involving electronic evidence.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic devices specified below (the "Subject Devices") for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice

received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESI”). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Devices

3. Subject Device-1 is particularly described as a silver Samsung phone with a silver case, inventoried by the FBI in connection with the arrest of MUSTAPHA RAJI on or about December 20, 2019.

4. Subject Device-2 is particularly described as a silver Samsung phone with a black case, assigned serial number R28J425GCTV, and inventoried by the FBI in connection with the arrest of MUSTAPHA RAJI on or about December 20, 2019.

5. Based on my training, experience, and research, I know that the Subject Devices have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs.

6. Based on my training and experience and the facts set forth above, I know that:

a. Cellular telephones like the Subject Devices frequently have voice mail and telephone directory features, as well as methods to learn the telephone number associated with each cellphone. Cellular telephones also typically contain records of recent call activity, both incoming and outgoing calls, and lists of stored telephone numbers and other identifying information, such as names.

b. Cellular telephones like the Subject Devices typically have voice mail and/or text-messaging features, which permit the cellphone user to send and receive voice mail and/or text

messages. Voice mail and text messages are typically stored on the computer network of the provider of the cellphone's telephone service, which network is external to the cellphone. Sent and received text messages may also be stored on the device.

c. Cellular telephones like the Subject Devices typically also have applications that enable the user to access and store email.

d. Cellular telephones with camera functions, like the Subject Devices, permit the cellphone user to take photographs and/or videos that are stored on the device.

e. The information described above usually remains accessible in the cellphone's memory card—or SIM card—even if the device loses battery power and/or has not been used for an extended period of time.

7. The Subject Devices are presently located in the Southern District of New York, secured in the custody of the FBI.

C. The Subject Offenses

8. For the reasons detailed below, I believe that there is probable cause to believe that the Subject Devices contain evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1343 and 1349 (wire fraud and conspiracy to do the same), 1956 (money laundering), and 2315 (receipt of stolen funds) (the "Subject Offenses").

II. Probable Cause

A. Probable Cause Regarding Subject's Commission of the Subject Offenses

9. On or about December 20, 2019, Indictment 19 Cr. 870 (JMF) was unsealed, charging the defendant, MUSTAPHA RAJI with (1) conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349, (2) wire fraud, in violation of Title 18, United States Code, Section 1343, (3) receipt of stolen funds, in violation of Title 18, United States Code, 2315,

and (4) money laundering conspiracy in violation of Title 18, United States Code, Section 1956(h).

The Indictment is attached hereto as Exhibit A and is incorporated by reference herein.

10. On or about September 15, 2018, RAJI's co-conspirator NANCY MARTINO-JEAN was charged in Complaint 18 Mag. 8070 (the "Complaint") filed in the Southern District of New York with wire fraud, in violation of Title 18, United States Code, Section 1343 and receipt of stolen funds, in violation of Title 18, United States Code, 2315.¹ The Complaint is attached hereto as Exhibit B and is incorporated by reference herein.

11. On or about December 20, 2019, RAJI was arrested by the FBI at a residence in the Southern District of Florida (the "RAJI Residence"). Prior to RAJI's arrest, the FBI had obtained a judicially-authorized order for prospective location information on a cellphone assigned call number [REDACTED] 5485 (the "5485 Phone"), and were obtaining location information on that phone. At the time of his arrest, the location information from the cellphone provider indicated that the 5485 Phone was located at the RAJI Residence,

12. Based on a conversation with an FBI agent present at the arrest of MUSTAPHA RAJI, I have learned the following in substance and in part:

- a. After his arrest, FBI agents accompanied RAJI as he got dressed and collected his medications.
- b. As FBI agents waited with RAJI in the kitchen-area of the RAJI Residence, RAJI stated, in sum and substance, that he would like to make a phone call.

¹ MARTINO-JEAN was later indicted and her case assigned to Honorable Naomi Reice Buchwald. *See* 18 Cr. 853 (NRB). MARTINO-JEAN has pleaded guilty and been sentenced.

- c. An arresting FBI agent observed the Subject Devices on the other side of the room, near a couch. The agent asked RAJI, in sum and substance, "Are these your phones?" RAJI responded in the affirmative.
- d. The arresting agents took RAJI, along with the Subject Devices, to an FBI office to complete the booking process. As part of the pedigree process, FBI agents asked RAJI for contact information for a friend or family member. RAJI identified a person and stated, in sum and substance, that the phone number for that person was contained in Subject Device-1. RAJI provided the PIN for Subject Device-1 to an FBI agent, who opened Subject Device-1, then handed Subject Device-1 to RAJI so that RAJI could read out the phone number. This same process was later repeated for a different contact person for RAJI.
- e. An arresting FBI agent turned off Subject Device-1, but was unable to turn off Subject Device-2. Based on the fact that the agent no longer received any location information from the 5485 Phone after turning off Subject Device-1, I believe that Subject Device-1 and the 5485 Phone are one and the same.
- f. FBI agents then inventoried the Subject Devices. Since the events described in Paragraph 14, the agents have not accessed either of the Subject Devices.

B. Probable Cause Justifying Search of the Subject Devices

13. Based on my training and experience and my familiarity with the investigation, I believe that MUSTAPHA RAJI participated in a scheme to fraudulently wire approximately \$1.7 million (the "Fraudulent Wire Transfer") to an account controlled by MARTINO-JEAN, who then received, transferred, and laundered stolen money.

14. During the course of the investigation of this case, I and other law enforcement officers have debriefed a cooperating witness (“CW-1”).² From my conversations with CW-1, I have learned the following, in substance and in part:

- a. RAJI provided the bank account information for a certain bank account (referred to in the Complaint as “Account-2”) to CW-1 and other co-conspirators, for the purpose of facilitating the \$1.7 million fraudulent wire transaction described in the Complaint.
- b. CW-1 had numerous text message conversations with RAJI, in or about September 2018, regarding the disbursement of fraudulently-obtained funds from Account-2.

I have viewed examples of those text message conversations on CW-1’s phone.

15. In addition, based on my training and experience, and my participation in this investigation, I know that participants in business email compromise schemes often maintain contact information relating to their criminal associates—including names, telephone numbers, direct connect numbers, and/or addresses—and store records relating to their illegal activity on electronic devices such as the Subject Devices. Such records can include, for example, logs of online “chats” with co-conspirators; email correspondence; contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and/or records of illegal transactions using false or stolen financial

² CW-1 has been charged with certain federal offenses and has proffered with the Government in the hopes of obtaining a cooperation agreement and leniency at sentencing. CW-1 has provided accurate and reliable information in the past, and this information has been corroborated by, among other things, my investigation in this matter.

and personal identification data. Individuals engaged in such criminal activity often store such records in order to, among other things, (1) keep track of co-conspirator's contact information; (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds for purposes of, among other things, dividing those proceeds with co-conspirators; and (4) store false or stolen data for future exploitation. In addition, participants in such schemes often use multiple phones for the purposes described above.

16. Accordingly, a search of the data on the Subject Devices would likely reveal contact information for criminal associates, including those who participated with RAJI and MARTINO-JEAN in fraud and money laundering activities, and would allow investigators to subpoena relevant phone records to find and identify those individuals. Moreover, the Subject Devices may contain sent or received electronic messages, as well as sent or received email messages, which reflect information regarding the commission of the Subject Offenses.

17. Computer files or remnants of such files can be recovered months or even years after they have been created or saved on an electronic device such as the Subject Devices. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. Thus, the ability to retrieve information from the Subject Devices depends less on when the information was first created or saved than on a particular user's device configuration, storage capacity, and computer habits.

18. Based on the foregoing, I respectfully submit there is probable cause to believe that RAJI is engaged in the Subject Offenses, and that evidence of this criminal activity is likely to be found on the Subject Devices.

III. Procedures for Searching ESI

A. Review of ESI

19. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained on the Subject Devices for information responsive to the warrant.

20. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

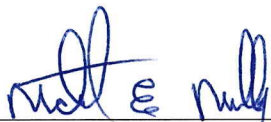
21. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement may need to conduct a complete review of all the ESI from the Subject Devices to locate all data responsive to the warrant.

B. Return of the Subject Device

22. If the Government determines that the Subject Devices are no longer necessary to retrieve and preserve the data on the device, and that the Subject Devices are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return the Subject Devices, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

IV. Conclusion and Ancillary Provisions

23. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.



Michael Mulloy
Task Force Officer, FBI

Sworn to before me on
February 19, 2020

S/Barbara Moses

HON. BARBARA C. MOSES
UNITED STATES MAGISTRATE JUDGE

Attachment A

I. Device Subject to Search and Seizure

The devices that are the subject of this search and seizure warrant (the “Subject Devices”) is described as follows:

- Subject Device-1 is particularly described as a silver Samsung phone with a silver case, (including any SIM Cards or other memory cards contained therein) inventoried by the FBI in connection with the arrest of MUSTAPHA RAJI on or about December 20, 2019.
- Subject Device-2 is particularly described as a silver Samsung phone with a black case, (including any SIM Cards or other memory cards contained therein) assigned serial number R28J425GCTV, and inventoried by the FBI in connection with the arrest of MUSTAPHA RAJI on or about December 20, 2019.

II. Review of ESI on the Subject Devices

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Devices for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1343 and 1349 (wire fraud and conspiracy to do the same), 1956 (money laundering), and 2315 (receipt of stolen funds) (the “Subject Offenses”), described as follows:

1. Evidence, including email communications, concerning the identity, or location of, the owner(s) or user(s) of the Subject Devices;
2. Evidence, including email communications, concerning the commission of business email compromises and spearphishing, including but not limited to the identity of co-conspirators and victims in connection with those offenses;
3. Evidence, including email communications, concerning the possession, receipt, use, transfer, or laundering of stolen funds, including but not limited to the identity of co-conspirators and victims in connection with those offenses;
4. Evidence, including email communications, concerning false or stolen identities and any accounts opened or maintained using such false or stolen identities, including but not limited to the identity of co-conspirators and victims in connection with those offenses;

5. Documents, spreadsheets and ledgers identifying and/or tracking victims, co-conspirators, stolen funds, and accounts used to receive, transfer, or launder stolen funds; and
6. Evidence concerning any online accounts or any electronic devices where evidence falling within the foregoing categories could be stored, including any passwords or encryption keys needed to access such evidence.